COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 43, No. 2 1994

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

Herbrand's Unit Theorem and Relative Units

by

Yoshitaka ODAI

(Received August 5, 1993)

Introduction

Let K be an algebraic number field with r_1 real places and r_2 complex places. Let L be a finite Galois extension of K. Then the following theorem is well known.

THEOREM (Herbrand [2, 3]). *There exist r_1+r_2 units of L whose conjugates over K generate a subgroup of the group of units of L of finite index.*

In this note we call the theorem *Herbrand's unit theorem*. We may restate Herbrand's unit theorem as follows.

THEOREM (Artin [1]). *There exist r_1+r_2 units of L which satisfy the following two conditions*:

(i) *Their relative norms to K are equal to* 1.

(ii) *Their conjugates over K together with a system of the fundamental units of K generate a subgroup of the group of units of L of finite index.*

It would be of some interest to consider Herbrand's unit theorem because, for example, a proof of the first fundamental inequality of class field theory needs it. In [4] we have defined and studied relative units. In this note, by using the results of [4], we shall improve Herbrand's unit theorem in the case that L/K is abelian. As an application we can somewhat improve the majoration of an index obtained in [5].

§1. Improvement of Herbrand's unit theorem for abelian extensions

Let $\boldsymbol{Q}$ (resp. $\boldsymbol{Z}$) denote the rational number field (resp. the ring of rational integers). Let K be a finite extension of $\boldsymbol{Q}$ with r_1 real places and r_2 complex places. Let L be a finite Galois extension of K of degree n and G the Galois group of L/K. For a subextension M of L/K, we denote by E_M (resp. W_M) the group of units of M (resp. the group of roots of unity in M) and define

$$E_{M/K}=\{\varepsilon\in E_M \mid N_{M/F}\varepsilon\in W_F \text{ for all proper subextensions } F \text{ of } M/K\},$$

where $N_{M/F}$ is the relative norm map for M/F. The elements of $E_{M/K}$ are called *relative*

units of M over K. We put $E=E_L/W_L$ and $\mathscr{E}_M=E_{M/K}W_L/W_L$.

Hereafter we assume that L/K is abelian. We put $\mathscr{E}=\prod_{M\in\mathscr{M}}\mathscr{E}_M$ where $\mathscr{M}$ denotes the set of cyclic subextensions of L/K. Then we have proved

LEMMA ([4]). (i) *$E^n\subset\mathscr{E}$ and the product $\prod_{M\in\mathscr{M}}\mathscr{E}_M$ is direct.*

(ii) *Let r_1^M be the number of real places of K which are unramified in M. Let $\mathfrak{O}_M$ denote the ring of integers of the $[M:K]$-th cyclotomic field and $\mathfrak{O}_M^{(m)}$ the direct sum of m copies of $\mathfrak{O}_M$. Then $\mathscr{E}_M$ is an $\mathfrak{O}_M$-module. Moreover,*

$$\mathscr{E}_M\cong\begin{cases}\boldsymbol{Z}^{(r_1+r_2-1)} & \text{if } M=K,\\ 0 & \text{if } M\neq K \text{ and } r_1^M+r_2=0,\\ \mathfrak{O}_M^{(r_1^M+r_2-1)}\oplus\mathfrak{A}_M & \text{if } M\neq K \text{ and } r_1^M+r_2>0,\end{cases}$$

where $\mathfrak{A}_M$ is a non-zero ideal of $\mathfrak{O}_M$.

The following improvement of Herbrand's unit theorem follows from Lemma.

THEOREM 1. *Let notations be as above. Let w be the order of W_L and r the rank of E. If L/K is abelian, then there exist r_1+r_2 units of L whose conjugates over K generate a subgroup of E_L of index not more than $wn^{2r}\prod_{M\in\mathscr{M}}c_M$, where c_M denotes the Minkowski constant of the $[M:K]$-th cyclotomic field. Moreover, if L/K satisfies the condition*

$$r_1^M\neq r_1 \quad \textit{for all} \quad M\in\mathscr{M}\setminus\{K\}, \tag{1}$$

then the number of the units can be replaced by r_1+r_2-1.

Proof. We have from (i) of Lemma that $[E:\mathscr{E}]$ is a divisor of n^r. There exists a non-zero ideal $\mathfrak{B}_M$ of $\mathfrak{O}_M$ such that $\mathfrak{A}_M\mathfrak{B}_M\cong\mathfrak{O}_M$ and the absolute norm of $\mathfrak{B}_M$ is not more than c_M. If $M\neq K$, then (ii) of Lemma implies that $\mathscr{E}_M$ has a submodule $\mathscr{F}_M$ such that $\mathscr{F}_M\cong\mathfrak{O}_M^{(r_1^M+r_2)}$ and $[\mathscr{E}_M:\mathscr{F}_M]$ is not more than c_M. Let $\boldsymbol{Z}[G]$ be the group ring of G over $\boldsymbol{Z}$, then, as stated in the proof of Proposition (iii) of [4], $\mathfrak{O}_M$ is a $\boldsymbol{Z}[G]$-module generated by an element. Hence $\mathscr{F}_M$ is a $\boldsymbol{Z}[G]$-module generated by $r_1^M+r_2$ elements. We denote a system of $\boldsymbol{Z}[G]$-generators of $\mathscr{F}_M$ by

$$\varepsilon_{M,i}\qquad(1\leq i\leq r_1^M+r_2).$$

On the other hand, (ii) of Lemma implies that $\mathscr{E}_K$ is generated by r_1+r_2-1 elements. We denote a system of generators of $\mathscr{E}_K$ by

$$\varepsilon_{K,i}\qquad(1\leq i\leq r_1+r_2-1).$$

Furthermore, we put

$$\begin{cases}\varepsilon_{M,i}=1 & \text{for } r_1^M+r_2<i\leq r_1+r_2 \text{ if } M\neq K,\\ \varepsilon_{K,r_1+r_2}=1.\end{cases}$$

We denote by $\langle * \rangle$ the module generated by $*$ over $\boldsymbol{Z}[G]$. As $[\mathscr{E}_M:\langle\varepsilon_{M,i}\,|\,1\leq i\leq r_1+r_2\rangle]$ is not more than c_M, we have that $[\mathscr{E}:\langle\varepsilon_{M,i}\,|\,M\in\mathscr{M},\ 1\leq i\leq r_1+r_2\rangle]$ is not

more than $\prod_{M\in\mathcal{M}} c_M$. We define

$$\varepsilon_i=\prod_{M\in\mathcal{M}} \varepsilon_{M,i} \qquad \text{for} \quad 1\leq i\leq r_1+r_2 .$$

As the definition of relative units and the calculation modulo W_L show that $N_{L/K}\varepsilon_i=\varepsilon_{K,i}^n$, we have $\varepsilon_{K,i}^n\in\langle\varepsilon_i\rangle$. For $N\in\mathcal{M}$, as $N_{L/N}\varepsilon_i=\prod_{K\subset M\subset N}\varepsilon_{M,i}^{[L:N]}$, we have $N_{L/N}\varepsilon_i^{[N:K]}=\varepsilon_{N,i}^n\prod_{K\subset M\subset N, M\neq N}\varepsilon_{M,i}^n$. It implies that $\varepsilon_{N,i}^n\in\langle\varepsilon_i\rangle$ if $\varepsilon_{M,i}^n\in\langle\varepsilon_i\rangle$ for all proper subextensions M of N/K. Then the induction proves

$$\langle\varepsilon_{M,i}\,|\,M\in\mathcal{M},\ 1\leq i\leq r_1+r_2\rangle^n\subset\langle\varepsilon_i\,|\,1\leq i\leq r_1+r_2\rangle .$$

Therefore we have that $[\langle\varepsilon_{M,i}\,|\,M\in\mathcal{M},\ 1\leq i\leq r_1+r_2\rangle:\langle\varepsilon_i\,|\,1\leq i\leq r_1+r_2\rangle]$ is a divisor of n^r. Having calculated modulo W_L, we know that $\{\varepsilon_i\}_{1\leq i\leq r_1+r_2}$ have the property in the theorem.

The condition (1) implies that $\varepsilon_{M,r_1+r_2}=1$ for all $M\in\mathcal{M}\backslash\{K\}$. Then we have $\varepsilon_{r_1+r_2}=1$ and can replace $\{\varepsilon_i\}_{1\leq i\leq r_1+r_2}$ by $\{\varepsilon_i\}_{1\leq i\leq r_1+r_2-1}$.

REMARK. (i) The index $[E:\mathscr{E}]$ has been more precisely studied in [5]. The constant c_M can be replaced by 1 if the class number of the $[M:K]$-th cyclotomic field is 1.

(ii) If the condition (1) is satisfied, then L/K is 2-elementary and $[L:K]\leq 2^{r_1}$.

For Artin's version, we have the following improvement.

THEOREM 2. *Let notations be as in Theorem* 1. *Let* r_1' *be the maximum of* r_1^M *for* $M\in\mathcal{M}\backslash\{K\}$. *If* L/K *is abelian, then there exist* $r_1'+r_2$ *units of* L *which satisfy the following two conditions*:

(i) *Their relative norms to* K *are equal to* 1.

(ii) *Their conjugates over* K *together with a system of the fundamental units of* K *generate a subgroup of* E_L *of index not more than* $w^{r+1}n^{2r}\prod_{M\in\mathcal{M}} c_M$.

Proof. We define

$$\varepsilon_i'=\frac{\varepsilon_i}{\varepsilon_{K,i}}=\prod_{M\in\mathcal{M}\backslash\{K\}}\varepsilon_{M,i} \qquad \text{for} \quad 1\leq i\leq r_1+r_2 .$$

As their relative norms to K are roots of unity, $\{\varepsilon_i'^w\}_{1\leq i\leq r_1+r_2}$ satisfy the conditions of the theorem. If $i>r_1'+r_2$, we have $\varepsilon_{M,i}=1$ for all $M\in\mathcal{M}\backslash\{K\}$. Therefore $\varepsilon_i'=1$ for $i>r_1'+r_2$ and the proof is complete.

REMARK. It is clear that $r_1'<r_1$ if and only if the condition (1) of Theorem 1 is satisfied.

§2. Application

In this section we assume that L/K is abelian. In [5] we have estimated the index $[E:\mathscr{E}]$. We put $\boldsymbol{E}=\prod_{M\in\mathcal{M}}\boldsymbol{E}_M$ where $\boldsymbol{E}_M$ is the subgroup of E consisting of

elements ε mod W_L such that $\varepsilon^\sigma \equiv \varepsilon \bmod W_L$ for all $\sigma \in Gal(L/K)$ and $N_{M/F}\varepsilon \in W_F$ for all proper subextensions F of M/K. It is clear that $\boldsymbol{E}$ containes $\mathscr{E}$. Let Q_G be the natural number defined by $\sqrt{n^{n-2}/\prod_{M\in\mathscr{M}} d_M}$ where d_M is the absolute value of the discriminant of the $[M:K]$-th cyclotomic field. By using Herbrand's unit theorem we have proved Theorem 4 of [5], which states that $[E:\boldsymbol{E}]$ is a proper divisor of $(nQ_G)^{r_1+r_2}$. Here, by using Theorem 1 we improve partially Theorem 4 of [5].

PROPOSITION. *If L/K is abelian and satisfies the condition* (1) *of Theorem 1, then $[E:\boldsymbol{E}]$ is a divisor of $(nQ_G)^{r_1+r_2-1}$. Moreover, $[E:\boldsymbol{E}] \neq (nQ_G)^{r_1+r_2-1}$ unless $n=2$ and $r_1^L = r_1 - 1$.*

Proof. Let $\{\varepsilon_i\}_{1\le i\le r_1+r_2-1}$ be as in the proof of Theorem 1. For $x=(x_1, x_2, \cdots, x_{r_1+r_2-1}) \in \boldsymbol{Z}[G]^{(r_1+r_2-1)}$ (the direct sum of r_1+r_2-1 copies of $\boldsymbol{Z}[G]$), we define $\rho(x) = \prod_{i=1}^{r_1+r_2-1} \varepsilon_i^{x_i} \bmod W_L$. Then ρ is a $\boldsymbol{Z}[G]$-homomorphism of $\boldsymbol{Z}[G]^{(r_1+r_2-1)}$ to E with $\boldsymbol{Z}$-torsion cokernel. Let $\mathfrak{B}$ denote the maximal order in the group ring $\boldsymbol{Q}[G]$ and $A^{\mathfrak{B}}$ the maximal $\mathfrak{B}$-lattice contained in a $\boldsymbol{Z}[G]$-module A. Then, by the same argument as in the proof of Theorem 4 of [5], we have that $[E:\boldsymbol{E}][ker\,\rho : (ker\,\rho)^{\mathfrak{B}}]$ is a divisor of $(nQ_G)^{r_1+r_2-1}$ and that the equation holds if and only if both E and $ker\,\rho$ are $\boldsymbol{Z}[G]$-projective. If $ker\,\rho$ is not $\boldsymbol{Z}[G]$-projective, then the equation does not hold. We assume that $ker\,\rho$ is $\boldsymbol{Z}[G]$-projective. Then $[ker\,\rho : (ker\,\rho)^{\mathfrak{B}}] = 1$ if and only if $ker\,\rho$ is trivial. Therefore we have $[E:\boldsymbol{E}] \neq (nQ_G)^{r_1+r_2-1}$ unless $ker\,\rho$ is trivial. The calculation of the $\boldsymbol{Z}$-rank of $ker\,\rho$ shows that $ker\,\rho$ is trivial if and only if $n=2$ and $r_1^L = r_1 - 1$. The proof is complete.

REMARK. If $n=2$ and $r_1^L = r_1 - 1$, it is possible that $[E:\boldsymbol{E}] = (nQ_G)^{r_1+r_2-1}$. For example, let K be a non totally real cubic field and L the Galois clousure of K. Then $n=2$, $r_1^L = r_1 - 1 = 0$ and L/K satisfies the condition (1) of Theorem 1. In this case Example 9 of [5] shows that $[E:\boldsymbol{E}] = (nQ_G)^{r_1+r_2-1} = 2$.

References

[1] ARTIN, E.; Über Einheiten relativ galoisscher Zahlkörper, *J. Reine Angew. Math.*, **167** (1931), 153–156.

[2] HERBRAND, J.; Nouvelle démonstration et généralisation d'un théorème de Minkowski, *C. R. Acad. Sci. Paris*, **191** (1930), 1282–1285.

[3] HERBRAND, J.; Sur les unités d'un corps algébrique, *C. R. Acad. Sci. Paris*, **192** (1931), 24–27.

[4] ODAI, Y.; On the group of units of an abelian extension of an algebraic number field, *Proc. Japan Acad. Ser. A*, **64** (1988), 304–306.

[5] ODAI, Y.; On the index of the group generated by relative units, J. Number Theory, **46** (1994), 60–69.

Gunma College of Technology
580 Toriba, Maebashi,
Gunma 371, Japan